

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark
Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 02 August 1999 (02.08.99)	
International application No. PCT/IB98/02139	Applicant's or agent's file reference PDC/AB/20309
International filing date (day/month/year) 23 December 1998 (23.12.98)	Priority date (day/month/year) 23 December 1997 (23.12.97)
Applicant TRANCHARD, Lionel et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

24 June 1999 (24.06.99)

☐ in a notice effecting later election filed with the International Bureau on:
2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Lazar Joseph Panakal

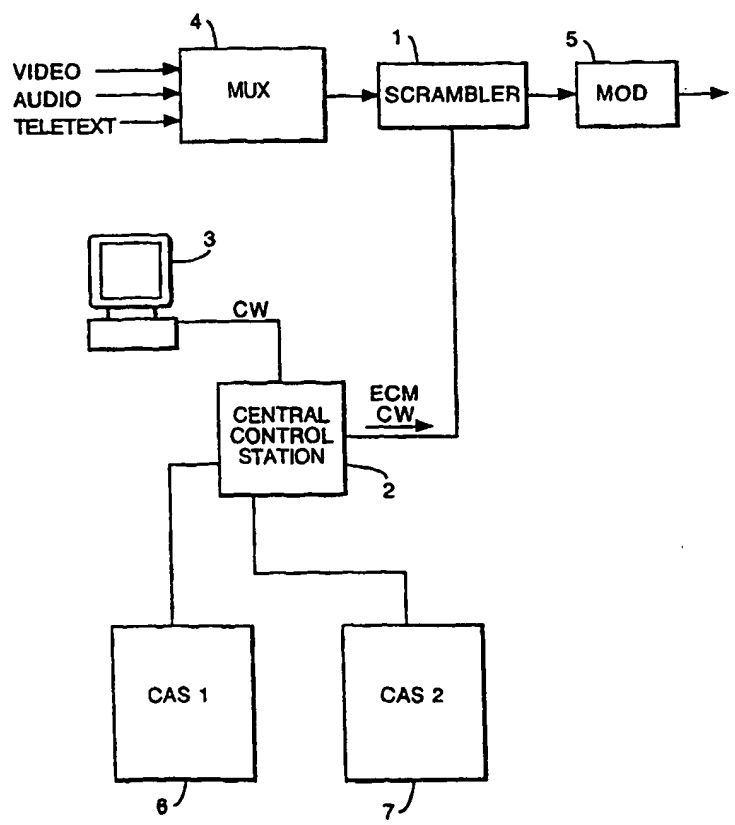
Telephone No.: (41-22) 338.83.38

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶: H04N 7/167	A1	(11) International Publication Number: WO 99/33271 (43) International Publication Date: 1 July 1999 (01.07.99)
(21) International Application Number: PCT/IB98/02139 (22) International Filing Date: 23 December 1998 (23.12.98) (30) Priority Data: 97403150.2 23 December 1997 (23.12.97) EP (71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai Andre Citroen, F-75711 Paris Cedex 15 (FR). (72) Inventors; and (75) Inventors/Applicants (for US only): TRANCHARD, Lionel [FR/FR]; 18, rue Martin Bernard, F-75013 Paris (FR). DE-CLERCK, Christophe [FR/FR]; 3, rue des Ormes Dancourt, F-28210 Senantes (FR). (74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published With international search report.
(54) Title: SCRAMBLING UNIT FOR A DIGITAL TRANSMISSION SYSTEM (57) Abstract <p>An independant scrambling unit (1) for a digital audiovisual transmission system, the scrambling unit (1) comprising an input for receiving an assembled transport packet stream from a physically sepeare multiplexer (4), a scrambling device for scrambling the received transport stream according to a randomising control word and an output for sending the scrambled transport stream to a transmitter means for subsequent transmission. The scrambling unit (1) may also be used to introduce other packet data in the data stream.</p>  <pre>graph LR VIDEO --> MUX[4] AUDIO --> MUX TELETEXT --> MUX MUX --> SCRAMBLER[1] SCRAMBLER --> MOD[5] SCRAMBLER --> CCS[2] CCS -- CW --> PC[3] CCS --> CAS1[6] CCS --> CAS2[7] CCS -- ECM CW --> SCRAMBLER</pre>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SCRAMBLING UNIT FOR A DIGITAL TRANSMISSION SYSTEM

The present invention relates to a scrambling unit for a digital audiovisual transmission system, in particular for a digital television transmission system, together with a
5 scrambling system including such a scrambling unit.

Transmission of scrambled or encrypted data is well-known in the field of digital pay TV systems, where scrambled audiovisual information is broadcast to a number of subscribers, each subscriber possessing a decoder or receiver/decoder capable of
10 descrambling the transmitted program for subsequent viewing.

Scrambling of the data is usually carried out by the multiplexing device also responsible for assembling the transmitted transport stream of data. The multiplexer receives digital video, audio or other digital data and assembles a single transport
15 packet stream. Each packet in the transport stream is usually of a predetermined length and contains a header and a payload.

The packet header includes a packet ID or PID identifying the packet and corresponding to the type of data (video, audio etc) within the packet. The payload
20 of the packet contains the audio, video or any other data such as application data processed by the receiver/decoder to provide extra functions, for example to generate a program guide etc.

Conventionally, the payload data is scrambled by a rapidly changing random control
25 word generated by the multiplexer. This control word is then sent to the receiver/decoder within an ECM, or Entitlement Control Message inserted in the transport packet stream in conjunction with the scrambled data. The ECM contains other information such as access rights and is itself encrypted by an appropriate encryption key before transmission.

30

The encrypted ECM is usually prepared by a separate access control system, proprietary to a particular channel or service provider. The access control system receives from the multiplexer the scrambling control word, inserts the control word in an ECM, encrypts the whole ECM with the current encryption key and sends the

- 2 -

encrypted ECM back to the multiplexer. The multiplexer then inserts the encrypted ECM in the transport stream together with the scrambled data.

5 The scrambled data and encrypted ECM are transmitted to a receiver/decoder having access to an equivalent of the encryption key so as to decrypt the ECM and thus obtain the control word to descramble the transmitted data. The exploitation key changes regularly and a decoder belonging to a paid-up subscriber will typically receive in a monthly EMM (Entitlement Management Message) the exploitation key necessary to decrypt the encrypted ECM for that month.

10

The advantage of scrambling the data with a control word generated by the multiplexer is that the system can be expanded to simultaneously scramble data for a number of access control systems in parallel. This may be necessary, for example, where the content provider is broadcasting to a mixed park of decoders, of different ages,
15 characteristics etc. Each access control system receives the control word used at that moment by the multiplexer and, thereafter, generates its own proprietary ECM, which is sent to the multiplexer for incorporation in the transport packet stream. Such "simulcrypt" systems use the same control word to scramble all data.

20 Whilst systems of this sort are relatively simple in terms of implementation, the management of communications between the multiplexer and the access control systems may be difficult to implement. Furthermore, the level of security is often limited by the complexity of the algorithm used by the multiplexer to generate the scrambling control word.

25

It is an object of the present invention in its various aspects and embodiments to overcome some or all of the problems of the prior art systems.

30 According to the present invention there is provided a scrambling unit for a digital audiovisual transmission system, the scrambling unit comprising an input for receiving an assembled transport packet stream from a physically separate multiplexer, a scrambling device for scrambling the received transport stream according to a randomising control word and an output for sending the scrambled transport stream to a transmitter means for subsequent transmission so as to permit the scrambling of

- 3 -

the transport packet stream by the scrambling unit independently of the multiplexer operations.

5 Unlike prior art systems, in which the scrambling of the data is carried out by the multiplexer at the same time as it multiplexes together the various data streams to form the single transport stream, the present invention proposes an entirely different solution in which a discrete scrambler unit receives via a dedicated input the already assembled transport stream.

10 This solution facilitates the management of communications between each of the elements of the system through the division of functionality between separated scrambling and multiplexing parts of the system. Furthermore, since the scrambling unit is not constrained by the usual limitations of multiplexer scrambler devices, the level of complexity of the scrambling algorithm can be increased.

15 The scrambling device may be adapted to carry out scrambling on some or all of the payload of selected packets of the transport stream packet. In a high "transport stream" scrambling level, all of the payload of a given transport stream packet may be scrambled, for example. Alternatively, only part of the payload of a packet may
20 be scrambled.

In addition to the scrambling device, the scrambling unit may also comprise a packet insertion means for inserting transport packet data in the transport stream. For example, the scrambling unit may be used to introduce packets containing the
25 scrambling control word within encrypted ECM messages. Other types of data may equally be inserted in the transport stream to make full use of available bandwidth, irrespective of the limitations of the multiplexer downstream of the unit.

In one embodiment, the packet insertion means may act to insert a packet of data in
30 the transport stream by detecting the presence of a null packet and replacing this packet by the packet to be inserted. A null packet is a packet generated during the operating cycle of the multiplexer that contains no data. It is conventionally identified by a characteristic PID value.

- 4 -

The scrambling unit may further comprise a packet filter means for identifying and copying to a memory part or all of a predetermined transport packet. For example, the filter may be pre-programmed to identify certain transport packets by their PID value that contain data to be modified by the scrambler, such as user specific tables or the like. Filtering may equally be carried out on part of a packet, e.g. by looking at the table ID within the payload of the transport packet etc.

Advantageously, the scrambling unit may also comprise a packet deletion means for deleting a predetermined packet, for example, transforming the packet ID of the packet to that of a null packet. For example, where the packet is to be filtered by its PID value and replaced by a modified packet with the same PID value, it will be necessary to delete the original packet with this PID to avoid generation of multiple packets with the same PID. The packet to be deleted will then become a null packet, which will thereafter be ignored or replaced another packet introduced by the packet insertion means.

Preferably, the scrambling unit also comprises a packet counting means for counting the number of packets of a predetermined packet ID value in the received transport data stream. For example, the packet counting means may be used to count the number of null packets in the data stream to enable evaluation of the space available in the transport stream to insert ECM packets etc. It may also be used to detect the presence of a particular packet ID or compute a bitrate of a packet ID.

Preferably, the scrambling unit also comprises a packet ID re-mapping means for changing the packet ID value assigned to a predetermined packet or set of packets. This may be used to remove the risk of any conflict between the PID value of an inserted packet and that of a packet already present in the transport stream by changing the PID value to one that does not occur in the incoming stream or to one that is filtered out.

The scrambling unit described above may operate in a stand alone mode. Alternatively, the unit may form part of a scrambling system, the system further comprising a central control means for generating a control word sent to and received by the scrambling unit for scrambling the transport stream. The central control means

- 5 -

may be implemented by a single PC, or a PC acting as a central control station in combination with a second PC and smart card for generating the control word.

5 Preferably, the scrambling system further comprises one or more access control systems connected to the central control means and adapted to receive a control word supplied by the central control means and to send back to the central control means an encrypted message e.g. an ECM message containing the control word.

10 In this manner the central control means can co-ordinate generation of an ECM based on the same control word by a plurality of access control systems, in accordance with the "simulcrypt" principle, and transmit the ECMs and their associated control word to the scrambler, for synchronised insertion of the ECMs in the transport stream and scrambling of the transport data in accordance with the control word.

15 Preferably, some or all of the data sent from the central control means to the scrambling unit is authenticated by the central control means by generation of a signature in accordance with a secret encryption key. In the case where a public/private encryption arrangement is used, the scrambling unit possesses an equivalent public key permitting the scrambler to verify the origin of the data. In
20 particular, all control word data sent to the scrambler should be authenticated, to avoid the possibility of falsification of the control word by breach of the connection between the two.

25 Further security measures may also be introduced, e.g. by encrypting all transmitted data in accordance with a symmetric algorithm, the central control means and scrambling unit each possessing the necessary keys for encryption and decryption of messages.

30 The embodiment of the scrambling system above has been described in relation to a single scrambling unit, a single central control means etc. However, for reasons of reliability it may be desired to have at least one stand-by or back up for each of the elements of the system and, in a preferred embodiment, the system comprises a plurality of scrambling units and associated central control means associated with the generation of the transport stream. In this way, the system may switch between

- 6 -

control means and scrambling units in the event of failure or erroneous operation of the relevant part of the system.

Advantageously, the or each scrambling unit in such a system is adapted to operate
5 autonomously in the event of disconnection from the central control means, for
example, by periodically storing its working configuration characteristics and/or
current control word value (or a default control word value).

In the context of the present application the term <<digital audiovisual transmission
10 system>> refers to all transmission systems for transmitting or broadcasting primarily
audiovisual or multimedia digital data. Whilst the present invention is particularly
applicable to a broadcast digital television system, the present invention may equally
be used in filtering data sent by a fixed telecommunications network for multimedia
internet applications etc.

15 The term MPEG refers to the data transmission standards developed by the
International Standards Organisation working group "Motion Pictures Expert Group"
and notably the MPEG-2 standard developed for digital television applications and set
out in the documents ISO 13818-1, ISO 13818-2, ISO 13818-3, and ISO 13818-4. In
20 the context of the present patent application, the term includes all variants,
modifications or developments of the basic MPEG formats applicable to the field of
digital data transmission.

There will now be described, by way of example only, a number of embodiments of
25 the present invention, with reference to the attached figures, in which:

Figure 1 shows the elements of a scrambling system of an embodiment of the
invention;

30 Figure 2 shows in detail the scrambling unit of Figure 1; and

Figure 3 shows a further embodiment of the present invention.

Referring now to Figure 1, there is shown a scrambling system for digital television

- 7 -

central control station 2 and a control word generator 3. The control word generator 3 may be, as shown, a PC type computer including a smart card reader adapted to receive a smart card containing an encryption key for signing data (see below). Alternatively, the control word generator may be a rack type unit, an add-on card to
5 be inserted in the control station 2 etc.

The scrambling unit 1 receives at its input unscrambled transport packets from a multiplexer 4 and passes a scrambled transport stream to a modulator 5 for preparation prior to transmission via a suitable satellite transmission link or the like.

10

The multiplexer 4 may be any conventional multiplexer conforming to the MPEG standard and capable of receiving digital video, audio, teletext etc information and producing a non-encrypted transport packet stream from this data. In a conventional MPEG broadcast system, video, audio etc data may be supplied to the multiplexer in
15 the form of a packetised elementary stream (PES). Other packet data may equally be multiplexed into the transport stream.

The output of the multiplexer comprises a sequence of transport packets comprising a header and a payload containing the PES or other data. Depending on the data
20 supplied to the multiplexer and the efficiency of the multiplexer, the packet stream may also comprise a greater or smaller number of so-called null packets containing no data.

Other types of data in the data stream provided to the multiplexer may be divided up
25 in sections. In addition or alternatively, data may also be provided to the multiplexer in the form of a number of tables or modules, the tables being downloaded and assembled by the receiver/decoder at the other end of the transmission system to form the complete application. In a similar manner to the packets in the transport packet stream, the tables may be identified by means of a table ID or TID value.

30

In the data stream, packets of data are identified by their packet ID or PID, video data having one PID value, audio data another etc. In the MPEG standard, null packets of data have the predetermined PID value of 0x1FFF. By way of contrast, the PID value assigned to a given type of data (audio, video etc) may be determined by the content

- 8 -

provider. For further details regarding the packet structure of an MPEG transport stream, the form of PES and sectioned and tabulated data, the reader is referred to the international standard documents ISO 13818-1, ISO 13818-2, ISO 13818-3, and ISO 13818-4. These standards also set out the characteristics of the physical interface layer
5 necessary to ensure compatibility between MPEG devices, and give as one example the use of an Asynchronous Serial Interface (ASI). Other links or interfaces are possible, for example, SPI, LVDS, G703 etc.

The modulator 5 may be of any conventional type necessary to convert the digital
10 transport packet stream into a form suitable for transmission via a telecommunications link such as a satellite, cable, network link etc.

The scrambling unit 1 is additionally connected to receive ECM and control word data from the central control station 2, which is in turn connected to the control word
15 generator 3 and one or more conditional access systems 6, 7. The control word generator 3 comprises a PC type computer capable of generating a randomised control word stream and including a card reader for reading a smart card containing a private key for signing the random control word data thus generated.

20 The central control station 2 may also comprise a PC or the like and, indeed, may even be integrated with the control word generator 3. In accordance with the principles of a "simulcrypt" system, the same control word is used to encrypt the transmissions for a number of access control systems. Each access control system encrypts the control word and other data with its own encryption key in order to
25 prepare an ECM message for broadcast to subscribers using this access control system.

The central control station 2 is therefore configured to pass the control word data via a suitable communications link to the access systems 6, 7 which prepare encrypted
30 ECM messages which are sent back to the central control station 2. The central control station 2 then sends the ECM messages (in the form of one or more transport packets) and associated control word data via, for example, a TCP/IP link to the scrambling unit 1.

- 9 -

- In order to avoid the possibility of the communication link being compromised and the control word data being substituted by other data originating outside of the system, the control word data is signed at the moment of generation by a private key held on the smart card associated with the generator 3, as described above. The scrambling unit 1 possesses an equivalent public key that may be used to authenticate the signed data, in accordance with known private/public key authentication methods. In the event that the control word data is not correctly authenticated, the scrambling unit may refuse to carry out scrambling of the transport packet stream.
- 10 Further encryption of communications passed between the control station 2 and scrambling unit 1 may also be carried out, for example, through the use of a symmetric encryption scheme and a pair of private keys held by the central control means and scrambling unit.
- 15 Referring now to Figure 2, the structure of the scrambling unit of Figure 1 will now be described in detail. As will be understood, some of the elements shown here represent functional blocks within the decoder that may be implemented in either hardware or software form or in a combination thereof.
- 20 The unit 1 receives via inputs 10, 11 the non-encrypted transport stream output from the multiplexer. In order to provide a degree of security against problems in the link between the multiplexer and the scrambling unit, a double connection is provided, as shown, with the same transport stream being received at each of the inputs 10, 11. The connection may also be used to manage redundancy of data streams originating from different multiplexer sources.
- 25

Information regarding the synchronisation and timing of the packets in the MPEG packet stream is provided to a central microprocessor 15 by the decoder and synchronisation elements 12, 13. The decoder and synchronisation elements detect that the data corresponds to an MPEG stream at a physical level (clock presence, correct ASI or other interface characteristics etc). The synchronisation element recovers the MPEG synchronisation byte to ensure subsequent synchronous processing of the data. These elements are conventional and are found, for example, in MPEG receiver/decoder units as an element of the decryption link.

30

- 10 -

In the event of any fault in the stream received via one of the inputs, the microprocessor controls a switching element 14 to change to the stream received via the other input. As will be seen, given the necessity to maintain a continuous flow of transmitted data, this sort of redundancy may be repeated at other levels in the scrambling system.

As will be described, the transport stream output via the outputs 18, 19 is normally scrambled. However, in order to provide an unscrambled and unaltered output from the unit, either for testing purposes or to bypass the scrambling circuitry in the event of a fault, the unit further includes emergency bypass switches 16, 17 manually operable and which enable the transport packet stream (received via either or both inputs) to be directly passed through the unit.

As shown by the cross-connection 20, the input/output link in the bypass mode may be switched such that the stream received via the input 10 emerges via the output 18, whilst that received via input 11 emerges via the output 19. Alternatively, by changing the configuration of the connection 20, input 10 may be connected to output 19 and input 11 to output 18. The cross-connection 20 may be implemented, for example, by external leads plugged into the unit, the configuration of which may be changed as desired. This cross-connection again enables verification of the individual communication channels to be more easily effected.

The advantage of such an implementation is that the bypass is completely passive such that the signal can pass through the unit, even in the case of a power failure. If activated by a relay, the bypass can be automatically activated when a power failure occurs.

The functioning of the elements of the PID counter 21, PID filter 22, PID deletion unit 23, PID re-mapping unit 24, packet insertion unit 25 and scrambler 26 will now be described. As will become clear, some of these elements such as the PID filter 22 and PID counter 21 are known in the context of a receiver/decoder where they are used in the demultiplexing and descrambling operations carried out on a received transport stream.

- 11 -

Similarly, the elements such as the scrambler 26, packet insertion unit 25, PID re-mapping unit 24 and PID deletion unit 23 are known in the context of a conventional combined multiplexer/scrambling device. Whilst there will therefore be no difficulty for one skilled in the art to assemble and construct these elements, it will nevertheless
5 be appreciated that the specific combination and juxtaposition of such elements in the context of an external unit as described is nevertheless entirely original.

The PID counter 21, programmable by the microprocessor 15 may be used to verify the presence or absence of packets with a predetermined PID value in the transport
10 packet stream as well as to count the number of packets bearing this PID value that are present in a given block of transport packets. In particular, the PID counter 21 may be used to count the number of null packets present in the transport stream (MPEG PID value: 0x1FFF) so as to evaluate the bit rate available for insertion of further packets (see below). Alternatively, the counter 21 may be used to detect the
15 presence of a packet such as a private data packet or the like which is to be modified or deleted by the unit.

In order to more fully analyse the data stream, a PID filter and demux unit 22 is used to filter out packet sequences of a given PID value and to copy these packets to the
20 memory 27. The filter unit 22 may also be used to carry out filtering at a lower level in the transport packet stream, for example, a filtering of sections and/or tables of data within the payload of a transport packet. As in conventional filter units used in a receiver/decoder, the filter 22 may be programmed to recognise table ID values, table ID extension values, section data etc.

25 The configuration of the filter 22 is set by the microprocessor 15, which is in turn connected via a network adapter 28 and a TCP/IP link to the central control station shown in Figure 2. The central control station can therefore choose which packets to filter out of the data stream.

30 An accessed or filtered packet in the data stream is copied by the filter 22 into the memory 27 associated with the microprocessor 15. The packet stored in the memory may then be transmitted via the TCP/IP link to the central control station for further analysis or modification. The central control station may decide, for example, to filter

out certain private data packets of a given PID value for modification or may require modification of the packets used to describe the contents of the transport stream in the event that entirely new packets with a new PID value are to be inserted in the transport stream.

5

As will be understood, the fact that a given packet has been filtered and copied into the memory does not mean that the packet has been physically removed from the transport stream. Accordingly, in the event that packets of a given PID value are to be inserted in the transport stream, it will be necessary to delete the present packets
10 having this value to avoid collision. In order to do this, the packet deletion unit is adapted to transform packets of a given PID value to null packets, by, inter alia, changing the PID value of the packets to the PID value of a null packet. Specifically, in the case of an MPEG standard packet, the following changes shall be carried out on the packet header:

15

PID value forced to 0x1FFF

Transport_scrambling_control forced to 00

Adaptation_field_control forced to 01

Payload_unit_start_indicator forced to 0

20

Continuity counter forced to 0 (optional).

As will be understood, null packets in the transport stream are not read since they supposedly contain no payload and the packets thus transformed are for all intents and purposes deleted. Furthermore, as will be described, the packet insertion unit 25 is in
25 fact adapted to detect and replace any null packets by packets held in the memory for insertion in the transport stream.

In addition and in the same way that the deletion unit 23 deleted certain PID packets to null packets by changing their PID value, a PID re-mapping unit may be provided
30 to change any given PID to a new PID value. This may be required to circumvent limitations of the original multiplexer that supplies the multiplexed transport stream to the scrambling unit and/or to avoid PID conflicts with new packets to be inserted into the transport stream. For example, the unit may be configured as follows:

- 13 -

	Incoming PID value	Re-mapped PID value
	0x20	0x0100
	0x21	0x0101
	0x22	0x0200
5	0x23	0x0201

Only the PID field in the transport packet header is modified. Transport packets not designated by these PID values remain unchanged. As with the deletion unit, the configuration of the PID re-mapping unit is in practice determined by the central control station. In the event that the packet insertion unit 25 has been programmed to insert packets of a PID value not present in the original transport stream, re-mapping of the PID values may not be necessary. In contrast, in the event that a potential conflict has been detected, the PID re-mapping unit will re-map the conflicting PID value in the original transport stream to a new value.

Turning now to the packet insertion unit 25, this unit is adapted to insert a transport packet held in the memory 27 to replace any null packet present in the transport stream. No change or management of the PID values of the inserted packets is effected by the unit 25. As mentioned above, potential PID conflicts are handled by the PID re-mapping unit 24 and the PID deletion unit 23.

Packets may be inserted in the transport stream in a number of different ways:

1. Cyclic data insertion. This may be used, for example, to introduce static tables of data. In this case, the packets are stored in a queue in the memory 27, a scheduler reading each of the queues at regular intervals to introduce the packet data in a cyclic fashion into the stream, a packet being introduced at each occurrence of a null packet. The scheduler handles the continuity counter (ie the sequential number of the packet) within the packet sequence to ensure the correct numbering of the transmitted sequence.

2. ECM synchronised insertion. In this case, ECM messages are received from the control station together with the associated control word data. The ECM messages are inserted as cyclic data, synchronised with the scrambling operation carried out by the

scrambler 26 using the control word data.

3. One shot data insertion. In this case, a packet sequence is inserted one time only in the transport stream. The sequence is stored in a FIFO queue in the memory, the
5 next packet in the queue being inserted at the occurrence of the next null packet. In this case, the continuity counter of the packets in the sequence may be pre-set before being received by the scrambling unit. One shot data insertion may be used to insert data received from the control station 2, or from other sources, such as EMM generators.

10

Packets or sequences of packets sent from the central control station 2 to the scrambling unit 1 in any of these operations may be identified with an associated identity value, such that the central control station can override or call-back the insertion of a packet or sequence of packets in the transport stream.

15

The transport packet stream, modified and including the desired ECM messages is then passed to the scrambler 26. The scrambler 26 may conform to a digital scrambler as used in any conventional multiplexer/scrambler device. In order to carry out scrambling of the transported data (but not of the ECM messages) the scrambler is
20 provided with the necessary PID information to prepare groups of packets having PID values indicating that they are to be scrambled.

Scrambling may be carried out at a transport stream level, i.e. on the whole of the payload of a transport packet, or (e.g. for audio/visual type data) at a PES stream
25 level, i.e. on the payload of the PES packets contained within the transport packets. Either type of scrambling may be desired according to the requirements of the service provider.

The scrambler carries out scrambling of the data according to the control word
30 provided by the central control station 1. As described above, the control word data is signed at the central control station by a private key and the control word and signature sent to the unit 1. The unit 1 includes a smart card reader adapted to read a smart card 29 containing the equivalent public key. At the same time as the control word is passed to the scrambler 26, the microprocessor 15 verifies the signature using

- 15 -

the public key, as shown. In the event that there is a failure in the authentication process, the scrambler 26 may be instructed to terminate the scrambling process or to ignore the control word that has been received.

- 5 As mentioned above, communications between the central control station and the scrambling unit may be further encrypted by means of a symmetric algorithm and, in this case, the smart card 29 may also contain the key necessary to decrypt communicated data before the authentication step.
- 10 In addition, in the case where the scrambling unit is adapted to receive data sent from other sources independent of the central control station (e.g. an EMM source), the network used to send messages from the central control station to the scrambling unit may be physically separate from the network used to receive messages received from other sources. In this case, the network adapter 28 will include two separate network
15 interfaces, the interface for receiving data from other sources being "read-only" to prevent the unit being re-programmed by sources external of the scrambling system.

As shown, the scrambling unit 1 further includes outputs 30, 31 to enable a clear transport stream output to be read from the unit. Unlike the output obtained by the
20 bypass switches 16, 17, the outputs 30, 31 represent the transport stream after modification by insertion/deletion of packets etc, but before scrambling is carried out. These outputs can be used for surveillance of the operation of the unit and monitoring of the result of the operations in clear. In addition, the unit may include a standard RS232 interface 32 to enable interrogation of the microprocessor for test purposes,
25 configuration out of network, or basic data insertion (file transfer capability) by terminal.

Figure 3 shows a further embodiment of the present invention, in which a number of the elements of the system of Figure 1 have been duplicated in order to provide a
30 degree of security through redundancy of the elements. In particular, a standby central control unit 2a and control word generator 3a together with a standby scrambling unit 1a have been indicated.

The parts of the access control systems concerned with generation of an ECM have

- 16 -

also been duplicated and this has been indicated by the reference numbers 6a, 7a. Audio, video etc signals may also be passed by a standby multiplexer 4a. Furthermore, a second transmission channel for generation of an MPEG transport channel may also be handled by the present system. This has been indicated by the
5 multiplexer 40 (and its standby 40a), scrambling unit 41 (and its standby 41a) and modulator 42.

The redundancy of the various elements in the system may be managed by a communication link between the control stations 2, 2a and/or a link to a supervisor or
10 remote terminal indicated by the line 43. In particular, a "heartbeat" signal may be provided from the station 2 to the station 2a, the control station 2a acting to take control of the generation of ECM messages and control word data in the event of any interruption of this signal. Similarly, the scrambler units 1, 1a may be slaved to the control stations to enable transfer of functions between the two in the event of failure
15 of one or the other scrambling unit.

In addition each scrambler unit 1,1a may be adapted to memorise e.g. in a FLASH memory the operating configuration of the unit and/or the control word value at predetermined intervals such that the units 1,1a may continue to operate in the event
20 of disconnection from the control stations 2,2a and/or after an interruption in the power supply.

Alternatively, a fixed predetermined configuration and control word value may put into memory, to be used in the event of disconnection and/or power down.

25

The configuration values can include details of packet Ids that the unit is meant to suppress or replace etc.

CLAIMS

1. A scrambling unit for a digital audiovisual transmission system, the scrambling unit
5 comprising an input for receiving an assembled transport packet stream from a
physically separate multiplexer, a scrambling device for scrambling the received
transport stream according to a randomising control word and an output for sending
the scrambled transport stream to a transmitter means for subsequent transmission, so
as to permit the scrambling of the transport packet stream by the scrambling unit
10 independently of the multiplexer operations.
2. A scrambling unit as claimed in claim 1 in which the scrambling device is adapted
to carry out scrambling on some or all of the payload of selected packets of the
transport stream packet.
- 15 3. A scrambling unit as claimed in claim 1 or 2 further comprising a packet insertion
means for inserting transport packet data in the transport stream.
4. A scrambling unit as claimed in claim 3 in which the packet insertion means
20 inserts a packet of data in the transport stream by detecting the presence of a null
packet and replacing a null packet by the packet to be inserted.
5. A scrambling unit as claimed in any preceding claim further comprising packet
filter means for identifying and copying to a memory part or all of a predetermined
25 transport packet.
6. A scrambling unit as claimed in any preceding claim further comprising packet
deletion means for deleting a predetermined packet or set of packets.
- 30 7. A scrambling unit as claimed in claim 6 wherein the packet deletion means deletes
a packet by transforming the packet ID of the packet to that of a null packet.
8. A scrambling unit as claimed in any preceding claim further comprising packet
counting means for counting the number of packets of a predetermined packet ID

- 18 -

value in the received transport data stream.

9. A scrambling unit as claimed in any preceding claim further comprising packet ID re-mapping means for changing the packet ID value assigned to a predetermined
5 packet or set of packets.

10. A scrambling system comprising a scrambling unit as claimed in any preceding claim together with central control means for generating a control word sent to and received by the scrambling unit for scrambling the transport stream.

10

11. A scrambling system as claimed in claim 10 further comprising one or more access control systems connected to the central control means and adapted to receive a control word supplied by the central control means and to send back to the central control means an encrypted message containing the control word.

15

12. A scrambling system as claimed in claim 10 or 11 in which some or all of the data sent from the central control means to the scrambling unit is authenticated by the central control means by generation of a signature in accordance with a secret encryption key.

20

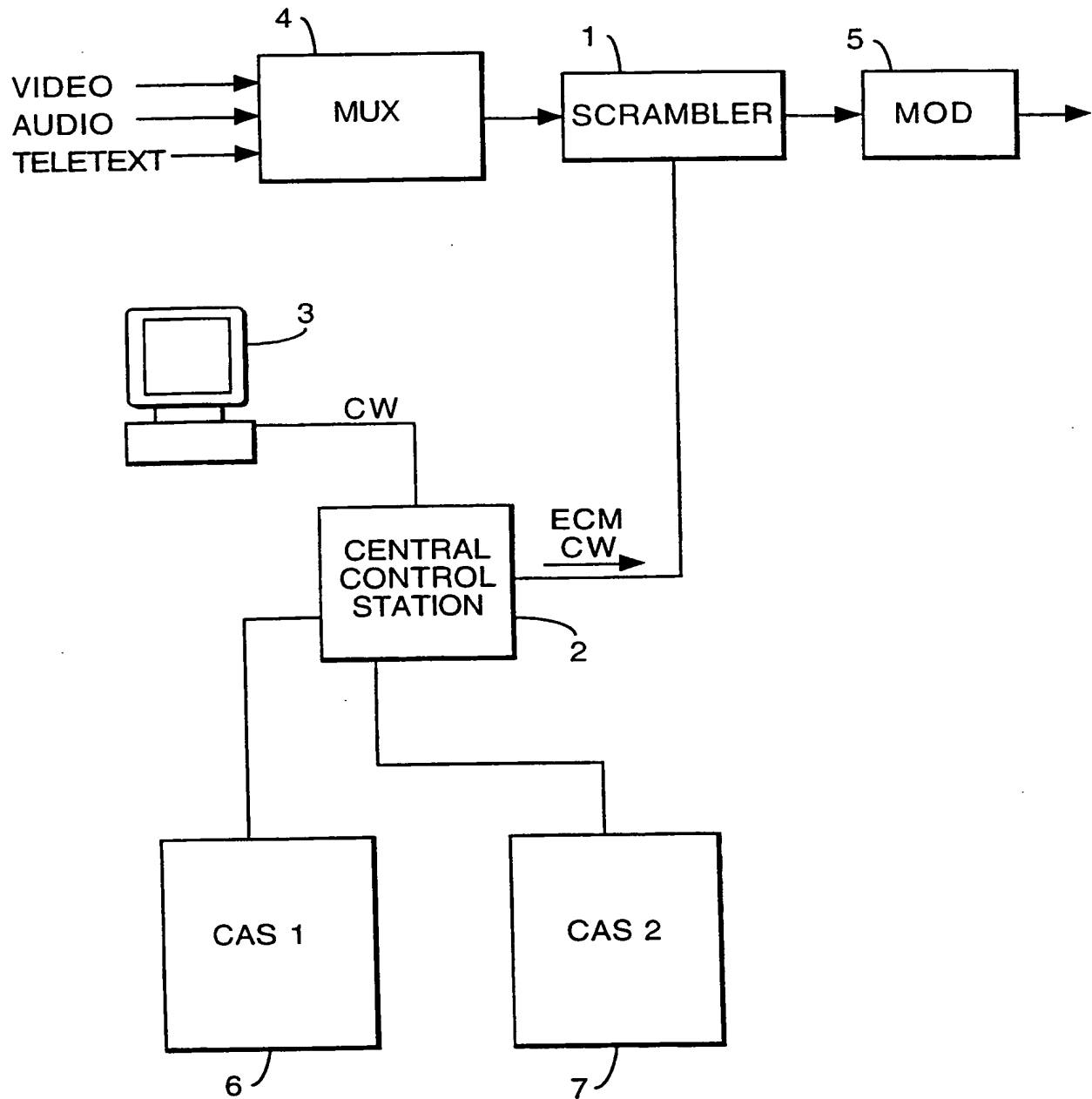
13. A scrambling system as claimed in any of claims 10, 11 or 12 comprising a plurality of scrambling units and associated central control means associated with the generation of a single transport stream.

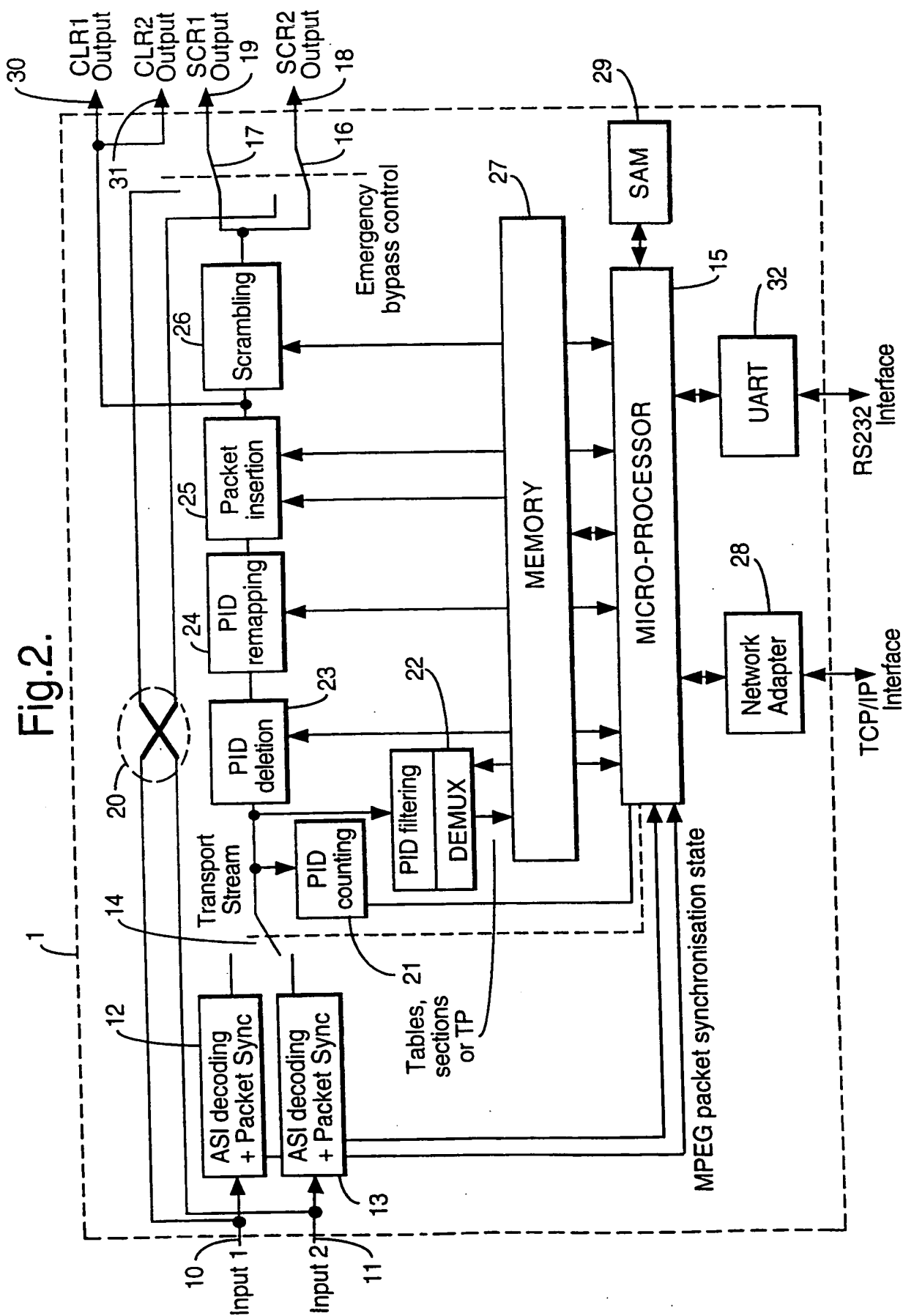
25 14. A scrambling system as claimed in any of claims 10 to 13 in which the or each scrambling unit is adapted to store its working configuration characteristics and/or the current control word value.

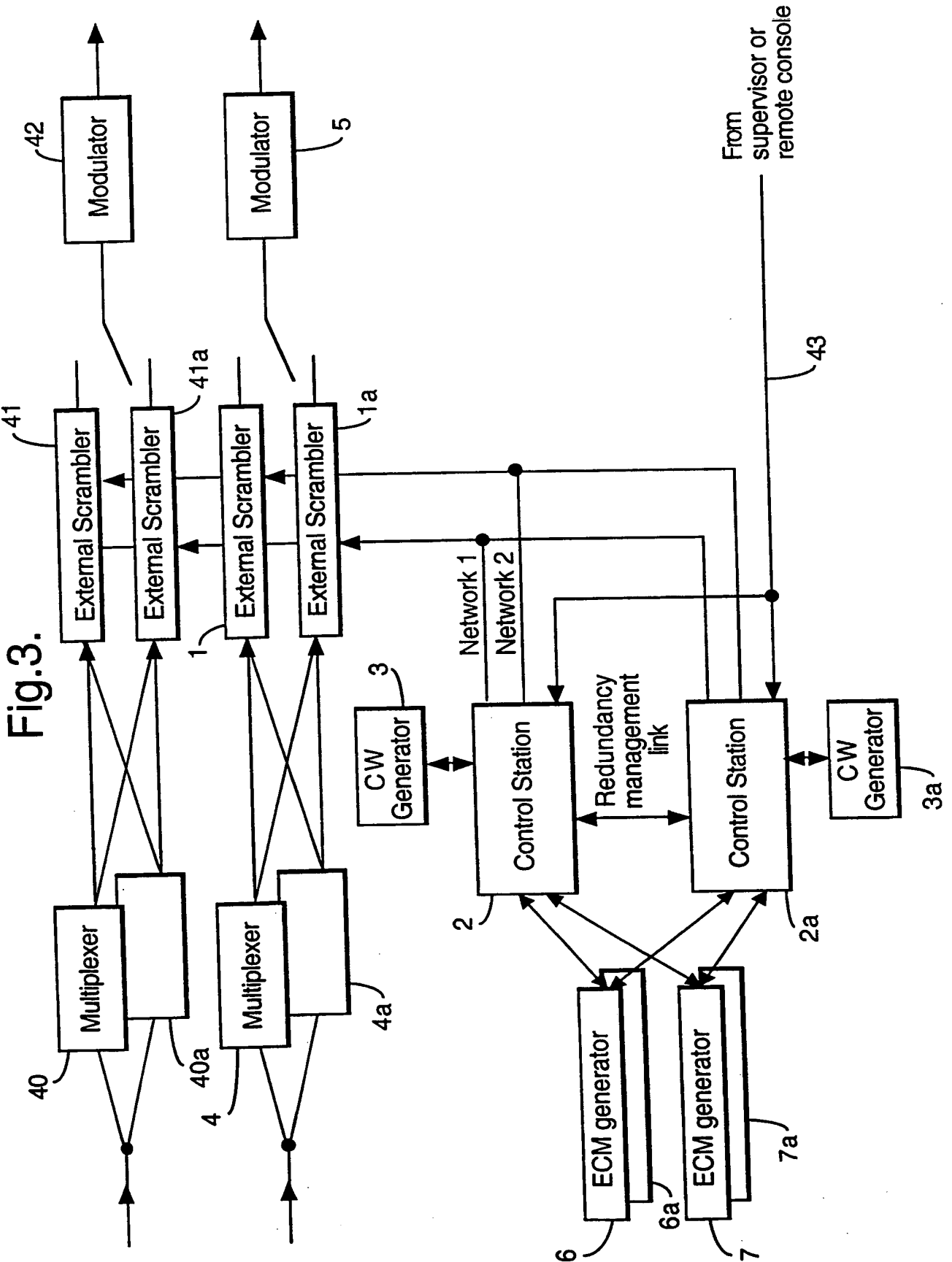
15. A scrambling unit substantially as herein described with reference to and as
30 illustrated in the accompanying drawings.

16. A scrambling system substantially as herein described with reference to and as illustrated in the accompanying drawings.

Fig.1.







INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PDC/AB/20309	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/IB 98/02139	International filing date (day/month/year) 23/12/1998	(Earliest) Priority Date (day/month/year) 23/12/1997
Applicant CANAL+ SOCIETE ANONYME et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☐ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1

☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 98/02139

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 762 765 A (HITACHI LTD) 12 March 1997 see page 3, column 3, line 47 - column 4, line 21 see page 4, column 5, line 6 - line 22 see page 4, column 16, line 19 - line 45 see figures 2-4,7 ---	1-3,8-16
A	GIACHETTI J -L ET AL: "A COMMON CONDITIONAL ACCESS INTERFACE FOR DIGITAL VIDEO BROADCASTING DECODERS" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 41, no. 3, August 1995, pages 836-841, XP000539543 NEW YORK, US see page 836, left-hand column, line 38 - page 837, left-hand column, line 8 see page 838, left-hand column, line 15 - right-hand column, line 30 --- -/--	1-3

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

30 March 1999

Date of mailing of the international search report

07/04/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Van der Zaai, R

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 98/02139

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>MICHON V ET AL: "HOW TO INTEGRATE ACCESS CONTROL MECHANISMS INTO DIGITAL HDTV SYSTEMS?" SIGNAL PROCESSING. IMAGE COMMUNICATION, vol. 4, no. 4 / 05, 1 August 1992, pages 421-428, XP000293758 AMSTERDAM, NL</p> <p>-----</p>	



PATENT COOPERATION TREATY



From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

MATHYS & SQUIRE
Attn. COZENS, P.
100 Gray's Inn Road
London WC1X 8AL
UNITED KINGDOM

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT
OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing
(day/month/year)

07/04/1999

Applicant's or agent's file reference

PDC/AB/20309

FOR FURTHER ACTION

See paragraphs 1 and 4 below

International application No.

PCT/IB 98/02139

International filing date
(day/month/year)

23/12/1998

Applicant

CANAL+ SOCIETE ANONYME et al.

1. ☒ The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after 18 months from the priority date, the international application will be published by the International Bureau.

If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 20 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority



European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Mustafa Corapci

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

PATENT COOPERATION TREATY

From the:
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
COZENS, P.
MATHYS & SQUIRE
100 Gray's Inn Road
London WC1X 8AL
GRANDE BRETAGNE

PCT

WRITTEN OPINION

(PCT Rule 66)

9/12/99
Reply Written Opin

Rep. CA - 9/10

Date of mailing (day/month/year)	09.09.99
-------------------------------------	-----------------

Applicant's or agent's file reference
PDC/AB/20309

REPLY DUE **within 3 month(s)**
from the above date of mailing

International application No. PCT/IB98/02139	International filing date (day/month/year) 23/12/1998	Priority date (day/month/year) 23/12/1997
--	---	---

International Patent Classification (IPC) or both national classification and IPC
H04N7/167

Applicant
CANAL+ SOCIETE ANONYME et al.

1. This written opinion is the **first** drawn up by this International Preliminary Examining Authority.
2. This opinion contains indications relating to the following items:
 - I ☒ Basis of the opinion
 - II ☐ Priority
 - III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain document cited
 - VII ☒ Certain defects in the international application
 - VIII ☐ Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

When? See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).


How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also: For an additional opportunity to submit amendments, see Rule 66.4.
For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis.
For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: **23/04/2000.**

Name and mailing address of the international preliminary examining authority:

 European Patent Office
D-80298 Munich
Tel. (+49-89) 2399-0 Tx: 523656 epmu d
Fax: (+49-89) 2399-4465

Authorized officer / Examiner

Schoeyer, M

Formalities officer (incl. extension of time limits)

Schmethüsen, S
Telephone No. (+49-89) 2399-2567 **8242**



I. Basis of the opinion

1. This opinion has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed".*):

Description, pages:

1-16 as originally filed

Claims, No.:

1-16 as originally filed

Drawings, sheets:

1/3-3/3 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. This opinion has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been and will not be examined in respect of:

- ☐ the entire international application,
☒ claims Nos. 15, 16,

because:

- ☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

WRITTEN OPINION

International application No. PCT/IB98/02139

- ☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 15, 16 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

- ☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

- ☐ no international search report has been established for the said claims Nos. .

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	No: 1,2,10
Inventive step (IS)	Claims	No: 3-9, 11-14
Industrial applicability (IA)	Claims	Yes: 1-14

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

III. Establishment of non-opinion

The subject-matter of claims 15 and 16 is so unclear that no meaningful examination can be performed. Although in this case the claims are directed towards a scrambling unit and a scrambling system respectively, none of the features of these claims are actually directed towards a unit or a system. It also seems in this case unnecessary to rely on references to the description and the figures (Rule 6.2(a) PCT).

V. Statement under Rule 66.2(a)(ii)

Reference is made to the following documents:

- D1: EP-A-0 762 765;
- D2: GIACHETTI J-L ET AL: "A COMMON ACCESS INTERFACE FOR DIGITAL VIDEO BROADCASTING DECODERS", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 41, no. 3, August 1995, pages 836-841;
- D3: MICHON V ET EL: "HOW TO INTEGRATE ACCESS CONTROL MECHANISMS INTO DIGITAL HDTV SYSTEMS ?", SIGNAL PROCESSING. IMAGE COMMUNICATION, vol. 4, no. 4 /05, 1 August 1992, pages 421-428.

Article 33(2) PCT

The application does not fulfil the requirements of Article 33(3) PC because the subject-matter of independent claim 1 is anticipated by D3. This will be set out below:

Document D3 is like claim 1 concerned with a scrambling unit for a digital audiovisual transmission system (see e.g. page 424, left column, line 14 ff..) and discloses:

a scrambling unit comprising an output for receiving an assembled transport packet stream from a physically separate multiplexer (see e.g. figure 2), a scrambling device for scrambling the received packet stream according to a randomising control word (see e.g. page 424, right column) and an output for sending the scrambled transport stream to a transmitter for subsequent transmission, so as to permit the scrambling of the transport packet stream by the scrambling unit independently of the multiplexer operations.

Since these are the technical features of claim 1, the subject-matter of this claim lacks novelty with respect to the document D3.

Dependent claims:

The subject-matter of dependent claims 2-14 lacks novelty or inventive because the features of these claims are either disclosed by prior art documents D1-D3 or form part

of the common general knowledge of the skilled person (as is also acknowledged by the applicants on the passage bridging pages 10-11 of the description of the application).

Lack of Novelty:

- scrambling of some or all of the payload (as in claim 2), -see D3 (page 423, paragraph 3.1);
- central control means for generating a control word (as in claim 10), -see D3 (page 423, paragraph 3.2 ff.);

Lack of Inventive Step:

- packet insertion means (as in claim 3), -see D1 (column 5, line 20);
- detection of nulls (as in claim 4), -common general knowledge;
- packet filter means (as in claim 5), -common general knowledge;
- deletion means (as in claims 6, 7), -common general knowledge;
- packet counting means (as in claim 8), -common general knowledge;
- ID re-mapping means (as in claim 9), -common general knowledge;
- access control systems (as in claim 11), -see D1 (column 1, line 24 ff.);
- authentication (as in claim 12), -see D1 (column 1, line 24 ff.);
- plurality of scrambling units (as in claim 13), -common general knowledge;
- scrambling unit is configured to store current control word (as in claim 14), -common general knowledge;

VII. Certain Defects

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 are not mentioned in the description.
2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
3. In order to facilitate the examination of the conformity of the amended application with the requirements of Article 34(2)(b) PCT, the applicant is requested to clearly identify the amendments carried out, no matter whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based (see also Rule 66.8(a) PCT).

PATENT COOPERATION TREATY

PCT

REC'D 09 MAR 2000

PO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PDC/AB/20309	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB98/02139	International filing date (day/month/year) 23/12/1998	Priority date (day/month/year) 23/12/1997
International Patent Classification (IPC) or national classification and IPC H04N7/167		
Applicant CANAL+ SOCIETE ANONYME et al.		


1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 24/06/1999	Date of completion of this report 07. 03. 00
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Schoeyer, M Telephone No. +49 89 2399 2136



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/IB98/02139

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

Description, pages:

1-16 as originally filed

Claims, No.:

1-16 as originally filed

Drawings, sheets:

1/3-3/3 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
☒ claims Nos. 15, 16.

because:



INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB98/02139

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 15, 16 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	3-9, 11-14
	No:	Claims	1,2,10
Inventive step (IS)	Yes:	Claims	
	No:	Claims	3-9, 11-14
Industrial applicability (IA)	Yes:	Claims	1-14
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

III. Establishment of non-opinion

The subject-matter of claims 15 and 16 is so unclear that no meaningful examination can be performed. Although in this case the claims are directed towards a scrambling unit and a scrambling system respectively, none of the features of these claims are actually directed towards a unit or a system. It also seems in this case unnecessary to rely on references to the description and the figures (Rule 6.2(a) PCT).

V. Statement under Article 35(2) PCT

Reference is made to the following documents:

- D1: EP-A-0 762 765;
D2: GIACHETTI J-L ET AL: "A COMMON ACCESS INTERFACE FOR DIGITAL VIDEO BROADCASTING DECODERS", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 41, no. 3, August 1995, pages 836-841;
D3: MICHON V ET EL: "HOW TO INTEGRATE ACCESS CONTROL MECHANISMS INTO DIGITAL HDTV SYSTEMS ?", SIGNAL PROCESSING. IMAGE COMMUNICATION, vol. 4, no. 4 /05, 1 August 1992, pages 421-428.

Article 33(2) PCT

The application does not fulfil the requirements of Article 33(3) PC because the subject-matter of independent claim 1 is anticipated by D3. This will be set out below:

Document D3 is like claim 1 concerned with a scrambling unit for a digital audiovisual transmission system (see e.g. page 424, left column, line 14 ff..) and discloses:

a scrambling unit comprising an output for receiving an assembled transport packet stream from a physically separate multiplexer (see e.g. figure 2), a scrambling device for scrambling the received packet stream according to a randomising control word (see e.g. page 424, right column) and an output for sending the scrambled transport stream to a transmitter for subsequent transmission, so as to permit the scrambling of the transport packet stream by the scrambling unit independently of the multiplexer operations.

Since these are the technical features of claim 1, the subject-matter of this claim lacks novelty with respect to the document D3.

Dependent claims:

The subject-matter of dependent claims 2-14 lacks novelty or inventive step because the features of these claims are either disclosed by prior art documents D1-D3 or form

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB98/02139

part of the common general knowledge of the skilled person (as is also acknowledged by the applicants on the passage bridging pages 10-11 of the description of the application).

Lack of Novelty:

- scrambling of some or all of the payload (as in claim 2), -see D3 (page 423, paragraph 3.1);
- central control means for generating a control word (as in claim 10), -see D3 (page 423, paragraph 3.2 ff.);

Lack of Inventive Step:

- packet insertion means (as in claim 3), -see D1 (column 5, line 20);
- detection of nulls (as in claim 4), -common general knowledge;
- packet filter means (as in claim 5), -common general knowledge;
- deletion means (as in claims 6, 7), -common general knowledge;
- packet counting means (as in claim 8), -common general knowledge;
- ID re-mapping means (as in claim 9), -common general knowledge;
- access control systems (as in claim 11), -see D1 (column 1, line 24 ff.);
- authentication (as in claim 12), -see D1 (column 1, line 24 ff.);
- plurality of scrambling units (as in claim 13), -common general knowledge;
- scrambling unit is configured to store current control word (as in claim 14), -common general knowledge;

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IB98/02139

VII. Certain Defects

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description.
2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
3. The independent claims have not been drafted in the two part form as stipulated by Rule 6.3(b) PCT.

PATENT COOPERATION TREATY

From the

INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

COZENS, P.
MATHYS & SQUIRE
100 Gray's Inn Road
London WC1X 8AL
GRANDE BRETAGNE

RECEIVED
MATHYS & SQUIRE

9 MAR 2000
REPLY DATE 7/4/2000
DIARY ENTERED

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT

(PCT Rule 71.1)

Date of mailing
(day/month/year)

07. 03. 00

Applicant's or agent's file reference
PDC/AB/20309

IMPORTANT NOTIFICATION

International application No.
PCT/IB98/02139

International filing date (day/month/year)
23/12/1998

Priority date (day/month/year)
23/12/1997

Applicant

CANAL+ SOCIETE ANONYME et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/

 European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer

Stannartz, B

Tel. +49 89 2399-8242



PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PDC/AB/20309	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) FOR FURTHER ACTION	
International application No. PCT/IB98/02139	International filing date (day/month/year) 23/12/1998	Priority date (day/month/year) 23/12/1997
International Patent Classification (IPC) or national classification and IPC H04N7/167		
Applicant CANAL+ SOCIETE ANONYME et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 7 sheets, including this cover sheet.

- ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 24/06/1999	Date of completion of this report 07. 03. 00
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Schoeyer, M  Telephone No. +49 89 2399 2136

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB98/02139

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-16 as originally filed

Claims, No.:

1-16 as originally filed

Drawings, sheets:

1/3-3/3 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
- ☒ claims Nos. 15, 16.

because:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/IB98/02139

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 15, 16 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	3-9, 11-14
	No:	Claims	1,2,10
Inventive step (IS)	Yes:	Claims	
	No:	Claims	3-9, 11-14
Industrial applicability (IA)	Yes:	Claims	1-14
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/<APPL>

III. Establishment of non-opinion

The subject-matter of claims 15 and 16 is so unclear that no meaningful examination can be performed. Although in this case the claims are directed towards a scrambling unit and a scrambling system respectively, none of the features of these claims are actually directed towards a unit or a system. It also seems in this case unnecessary to rely on references to the description and the figures (Rule 6.2(a) PCT).

V. Statement under Article 35(2) PCT

Reference is made to the following documents:

- D1: EP-A-0 762 765;
- D2: GIACHETTI J-L ET AL: "A COMMON ACCESS INTERFACE FOR DIGITAL VIDEO BROADCASTING DECODERS", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 41, no. 3, August 1995, pages 836-841;
- D3: MICHON V ET EL: "HOW TO INTEGRATE ACCESS CONTROL MECHANISMS INTO DIGITAL HDTV SYSTEMS ?", SIGNAL PROCESSING. IMAGE COMMUNICATION, vol. 4, no. 4 /05, 1 August 1992, pages 421-428.

Article 33(2) PCT

The application does not fulfil the requirements of Article 33(3) PC because the subject-matter of independent claim 1 is anticipated by D3. This will be set out below:

Document D3 is like claim 1 concerned with a scrambling unit for a digital audiovisual transmission system (see e.g. page 424, left column, line 14 ff..) and discloses:

a scrambling unit comprising an output for receiving an assembled transport packet stream from a physically separate multiplexer (see e.g. figure 2), a scrambling device for scrambling the received packet stream according to a randomising control word (see e.g. page 424, right column) and an output for sending the scrambled transport stream to a transmitter for subsequent transmission, so as to permit the scrambling of the transport packet stream by the scrambling unit independently of the multiplexer operations.

Since these are the technical features of claim 1, the subject-matter of this claim lacks novelty with respect to the document D3.

Dependent claims:

The subject-matter of dependent claims 2-14 lacks novelty or inventive step because the features of these claims are either disclosed by prior art documents D1-D3 or form

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/<APPL>

part of the common general knowledge of the skilled person (as is also acknowledged by the applicants on the passage bridging pages 10-11 of the description of the application).

Lack of Novelty:

- scrambling of some or all of the payload (as in claim 2), -see D3 (page 423, paragraph 3.1);
- central control means for generating a control word (as in claim 10), -see D3 (page 423, paragraph 3.2 ff.);

Lack of Inventive Step:

- packet insertion means (as in claim 3), -see D1 (column 5, line 20);
- detection of nulls (as in claim 4), -common general knowledge;
- packet filter means (as in claim 5), -common general knowledge;
- deletion means (as in claims 6, 7), -common general knowledge;
- packet counting means (as in claim 8), -common general knowledge;
- ID re-mapping means (as in claim 9), -common general knowledge;
- access control systems (as in claim 11), -see D1 (column 1, line 24 ff.);
- authentication (as in claim 12), -see D1 (column 1, line 24 ff.);
- plurality of scrambling units (as in claim 13), -common general knowledge;
- scrambling unit is configured to store current control word (as in claim 14), -common general knowledge;

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/<APPL>

VII. Certain Defects

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description.
2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
3. The independent claims have not been drafted in the two part form as stipulated by Rule 6.3(b) PCT.